Journal of Industrial Information Integration 47 (2025) 100902

Contents lists available at ScienceDirect

Journal of Industrial Information Integration

journal homepage: www.elsevier.com/locate/jii

Full Length Article

Blockchain-based cloud controllers for reliable networked control systems

Zhongcheng Lei [a], Luis de la Torre [b,*], Francisco-José Mañas-Álvarez [b], Wenshan Hu [a]

[a] Department of Artificial Intelligence and Automation, Wuhan University, China
[b] Department of Computer Sciences and Automatic Control, Universidad Nacional de Educación a Distancia, Spain

ARTICLE INFO

Keywords:
Blockchain
Controller failure
Cloud control
Smart contract
Event-based control

ABSTRACT

Networked control systems are critical in industrial applications but remain vulnerable to controller failures, which can destabilize operations. Blockchain technology offers a decentralized solution to enhance reliability. While blockchain technologies have been mainly used in financial systems (such as cryptocurrencies) so far, they are now being used in an increasing number of applications (such as logistics, power grids, or the Internet of Things) due to their powerful features and advantages. In this article, the use of blockchains is proposed and explored to deploy decentralized and reliable controllers. A blockchain-based controller architecture is presented to provide controllers that are permanently available, open accessible, and open source. Time to transaction finality and cost for transactions are analyzed in different blockchain networks, thus identifying their suitability. Our analysis reveals that blockchain networks can potentially be applied in slow processes with big enough time constants. Moreover, we propose the integration of event-based control to reduce transaction costs, thereby enhancing the viability of blockchain technologies in networked control systems. To demonstrate the practical application and cost efficiency of our approach, we present a case study focusing on a greenhouse climate control system. Results show that feasible blockchain networks – those compatible with sampling period constraints – consistently reduce control costs. For instance, on Fantom blockchain, event-based control achieved a 27.73-fold reduction in average control costs across six system variables over the eight-day operation period.

1. Introduction

Networked control systems (NCSs) are feedback control systems whose control loops are closed through communication networks. As NCSs are important in industrial applications, numerous studies have been performed to address the issues brought about with the introduction of communication networks compared to traditional control systems, such as communication constraints (e.g., time delay and data dropouts), controller failure [1–3], and event-triggered control [4].

In an NCS, a controller can be placed on the plant side, on the client side, or in the cloud, as shown in Fig. 1 [5]. Controller failure can occur due to various environmental factors [1], degrade system performance and can even lead to system instability and cause terrible results in engineering scenarios, especially for control systems in critical infrastructures [2,3]. Several approaches have been proposed to address the issues of controller failure. In [2], it was proven that in symmetric H_∞ control systems, if the unavailability rate of the controller is small enough, the exponential stability of the system can be preserved to some extent, even with controller failure. In [1], the theory of switched delay systems was used to tackle controller failure in a system with delays.

A different approach to ensure a reliable controller is using a cloud control system architecture, in which the controller is put in the cloud and called "cloud controller" [6]. Fig. 2 illustrates the architecture of a cloud control system, in which users access the control service provided by the cloud. A cloud control system has various merits. For example, it can take advantage of integrated cloud services that require little to no maintenance, reducing the possibilities of suffering controller failure due to blackouts or power surges, and thus, being more reliable than conventional control systems. However, the architecture shown in Fig. 2 does not fully mitigate the risks of controller failure or malicious attacks, such as denial of service (DoS) attacks. Even for a small failure time interval, the consequences may still be unacceptable. Backup / replicated servers (for the Nginx and business clusters in Fig. 2, for example) help increase security and reduce the previous risks. Nevertheless, cloud services and access points sometimes fail and cease to be available for some time, bringing down the whole service during those periods of time. For these reasons, blockchain technologies can provide an advantage worth considering.

As a disruptive technology due to its decentralization, security, and immutability features, blockchain has primarily been used in financial

* Correspondence to: Department of Computer Sciences and Automatic Control, Universidad Nacional de Educación a Distancia, Madrid 28040, Spain.
E-mail address: ldelatorre@dia.uned.es (L. de la Torre).

https://doi.org/10.1016/j.jii.2025.100902
Received 24 May 2023; Received in revised form 27 June 2025; Accepted 2 July 2025
Available online 14 July 2025

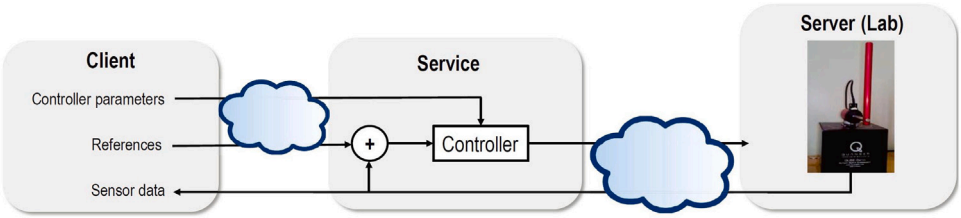

Fig. 1. Control architecture where the controller is in the cloud.

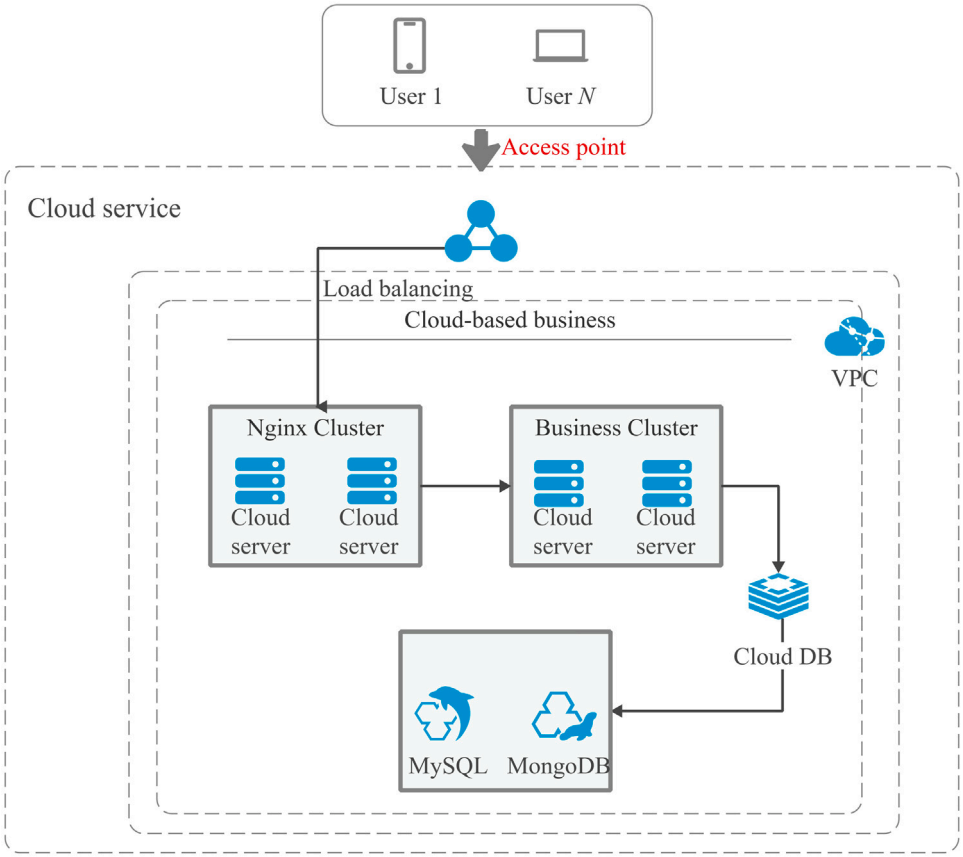

Fig. 2. Architecture of the cloud control system.

systems (such as cryptocurrencies) so far. However, it is now being increasingly used for other applications, such as supply chains using blockchain smart contracts [7], Industry 4.0 applications [8,9], power grids with privacy-preserving and efficient aggregation [10], or the Internet of Things (IoTs) for secure and trustworthy operations [11]. Beyond its broader applications in securing cyber–physical systems [12, 13], blockchain technology has also been explored within NCSs, primarily to ensure data security and integrity against cyber-attacks, which are critical concerns for reliable industrial information integration. Examples include leveraging distributed ledgers for the NCS infrastructure [14,15] and implementing secure control mechanisms to mitigate false data injection attacks in NCSs [16].

As computing resources, energy consumption (for example, for an IoT sensor), and bandwidth are sometimes limited in NCSs, and blockchain networks have their own limitations (in terms of speed and costs), we propose adding one missing ingredient to the mix. Event-triggered control, or event-based control (EBC), in which the event generates signals to close the control loop, can be useful in these scenarios [5], as these techniques can produce efficient control signals compared to time-based periodic sampling, without degrading the system performance too much [4].

For such applications, reliability, security, control performance (such as timely response), and the cost of control should be considered. Previous studies have investigated lightweight blockchain architectures [17] and the integration of artificial intelligence (AI) and blockchain for reliable, real-time decision-making in IoT-centric environments [18]. In this article, a blockchain-based controller is proposed to address the issues of control reliability and security with reasonable performance and cost in NCSs. While blockchain-based controllers are a type of cloud controller, the difference is that the former is hosted and run on a decentralized network, whereas the latter does not specify whether it is hosted and run on a centralized or a decentralized infrastructure. To illustrate the practical application and benefits of our proposed blockchain-based NCS with EBC, we present a case study focused on a greenhouse climate control system as a real-world scenario. The greenhouse system monitors six key variables: inside temperature, outside temperature, humidity, solar radiation, wind speed, and wind direction. In our blockchain-based NCS, we implement a send-on-delta EBC method, which triggers data transmission only when a significant change in the value of a variable occurs. This approach significantly reduces the number of blockchain

transactions needed, thereby optimizing costs while maintaining system performance. For instance, on the Fantom blockchain, the EBC achieves a 27.73-fold reduction in average control costs across six system variables over the eight-day operation period.

The rest of the article is organized as follows. In Section 2, the related work on blockchain and smart contracts is outlined. Section 3 presents the architecture, design, advantages and disadvantages of blockchain-based cloud controllers. A discussion on possible systems where the proposed architecture can be used can be found in Section 4, along with an estimation of the costs, depending on the blockchain network where the controller is deployed, and on whether EBC techniques are used or not. Finally, Section 5 includes an application example, while Section 6 presents our conclusions.

2. Related work

In this section, a brief introduction to distributed ledger technology (DLT), directed acyclic graphs (DAGs), blockchain, smart contracts and related works is included.

DLT is a ledger that is held by multiple actors in a distributed way. A blockchain is a type of DLT, an electronic ledger, that stores transactions distributedly and duplicately on all computers throughout the blockchain network. Each computer in the network is called a node and stores a copy of the transactions. DAGs are another form of DLT that can provide better performance in terms of transaction fees and speed than blockchains. IOTA is an example of a DAG that enables parallel processing of transactions and is designed for IoT use cases with transactions between networked physical devices [19].

As the name indicates, a blockchain is formed by linearly chained blocks, with the latter block chained to the former one. Fig. 3 illustrates a schematic of a blockchain with three blocks. Each block contains data (normally transaction records), the hash of the former block, and its own hash. For example, *Block* i contains the transactions (data), the hash (*Hash* $i-1$) of the previous *Block* $i-1$, and its own hash (*Hash* i).

Blockchain is a crucial technology to enable secure and distributed/decentralized data organization, which was first proposed and used in Bitcoin cryptocurrency in 2009 [20]. In 2013, Ethereum was proposed, providing the Ethereum virtual machine (EVM), which can be used as a platform for other technologies to build on. Ethereum was the first blockchain to support smart contracts, pieces of code inside a blockchain that can be executed automatically when certain conditions are met [21]. The introduction of smart contracts on blockchains broadens the potential applications of this technology, from cryptocurrencies to finance [22], IoT [23], and energy scenarios [24], which has attracted increasing research interest.

Common blockchain networks (including Bitcoin, Ethereum, Solana, and Polygon), as well as newer ones (such as Fantom, Zenith, Casper, and WAX), which are not yet popular, are analyzed in this article for the purpose of NCS applications. Table 1 shows different blockchain networks and their main features.

In a blockchain network, the consensus algorithm is vital for deciding whether a block is added to the chain. Bitcoin uses proof-of-work (PoW) to reach consensus [20], which means calculating the hash of the block based on computational capabilities (called mining). PoW requires computing power; thus, it implies the consumption of a large amount of energy [25]. Therefore, new types of consensus algorithms, such as proof of stake (PoS) [26], have been proposed to address the issue of energy consumption. Different blockchains have proposed different variants of PoS, such as asynchronous Byzantine fault tolerance (aBFT), practical Byzantine fault tolerance (pBFT) and tower Byzantine fault tolerance (tBPF).

To increase the scalability of blockchains, the concept of layers, or levels, was proposed. Layer-1 blockchains (such as Bitcoin, Ethereum, or Solana) usually adopt different consensus algorithms, whereas layer-2 blockchains are based on a layer-1 blockchain. For example, Polygon is a layer-2 blockchain technology that is based on Ethereum, thus, the merits of Ethereum (like, for instance, its security) can be inherited, while the network scales with higher transaction speeds. Another solution to increase scalability in level-1 blockchain networks is called sharding, which divides the blockchain into separate shards so that nodes can process the transactions assigned to them in parallel [27].

Blockchain networks are a formidable candidate to provide reliable controller services due to their distributed and replication features. In [15], a blockchain-based communication structure was proposed to address the potential cyberattacks in NCSs to ensure the security and stability of NCSs. In [28], Ethereum smart contracts were used for secure end-to-end encryption for defeating man-in-the-middle attacks. Currently, there are attempts to integrate blockchain for controllers, which are related mainly to software defined networks (SDNs) [29], where the controller is not in the blockchain.

Several studies have explored blockchain integration in industrial systems, primarily focusing on enhancing data integrity, traceability, and decentralized infrastructure. In [11], a lightweight blockchain framework was introduced to improve security and trust in industrial IoT systems, particularly in device-level access control and consensus mechanisms. While the work in [11] demonstrated blockchain's utility for secure data exchange, our study advances this by using blockchain as an execution layer for closed-loop industrial control systems, addressing timing and cost challenges in control logic deployment, which are critical for Industry 4.0 integration.

A broader analysis by [8] developed a WHY-HOW-WHAT framework to evaluate blockchain's role in Industry 4.0, covering areas like supply chains, maintenance, and digital manufacturing. Notably, the review identifies a lack of research on blockchain for real-time decision-making. Our work bridges this gap by investigating blockchain's feasibility in NCSs, especially under sampling-period limits, and by proposing event-based control to reduce transaction costs.

The approach presented in [30] employed non-fungible tokens (NFTs) and digital twins to track unmanned aerial vehicle (UAV) part certifications via smart contracts. Although their method ensures product authenticity, we focus on live system integration, demonstrating how blockchain-based smart contracts can facilitate decentralized control in NCSs. Both approaches leverage blockchain for transparency and trust, but our work uniquely applies it to dynamic control rather than static asset tracking.

Collectively, these studies underscore blockchain's capacity to enhance transparency and decentralization in industrial systems. Our work advances this field by introducing a cost-efficient, event-based control system that uses blockchain's immutability and openness to enable autonomy in latency-tolerant industrial processes. By proposing a blockchain-based cloud controller architecture, this work contributes to the development of more secure, reliable, and trustworthy frameworks for industrial information integration within NCSs.

These fundamental properties of blockchain (immutability, decentralization, and resilience) open up new opportunities in industrial automation and control systems.

3. Proposal and analysis

Having established the fundamental properties and potential of blockchain networks, this section focuses on our specific proposal: a blockchain-based controller architecture. This approach leverages smart contracts deployed on decentralized blockchain platforms to achieve enhanced reliability, fault tolerance, and transparency in cloud-based networked control systems. The following subsections address all the key aspects in this regard.

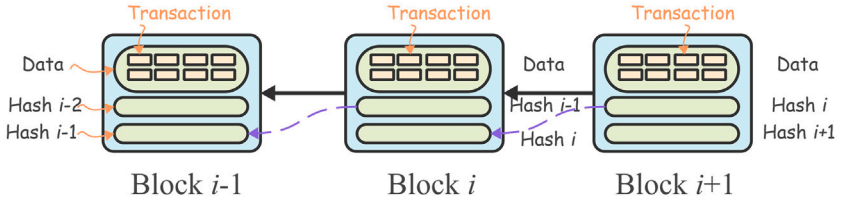

Fig. 3. Schematic of a blockchain with three blocks.

Table 1
Different blockchain networks and their main features.

Blockchain name	Created year	Blockchain/DAG	Consensus algorithm	Blockchain scalability	Main features
Bitcoin [20]	2009	Blockchain	PoW	Layer 1	The first public and open-source blockchain technology
Ethereum [26]	2013	Blockchain	PoS	Layer 1	Introducing smart contracts and providing EVM
IOTA [19]	2015	DAG	Fast probabilistic consensus	Layer 2	Being lightweight to allow its protocol to run on edge devices, especially for IoT use cases
Solana [31]	2017	Blockchain	PoS (tBFT) & PoH	Layer 1	High speed of transactions and small block time
Polygon [32]	2017	Blockchain	PoS	Layer 2	Uses sidechains that run alongside the Ethereum main chain
WAX [33]	2017	Blockchain	Delegated Proof of Stake (DPoS)	Layer 1	Mainly designed for e-commerce transactions
Fantom [34]	2018	DAG	PoS (Lachesis aBFT)	Layer 1	Leaderless PoS protocol
Casper [35]	2021	Blockchain	PoS (Highway Protocol)	Layer 1	Energy-efficient model and predictable gas fees
Zenith [36]	2022	Blockchain	Proof of Authority	Layer 1	Supports lower fees to generate blocks faster

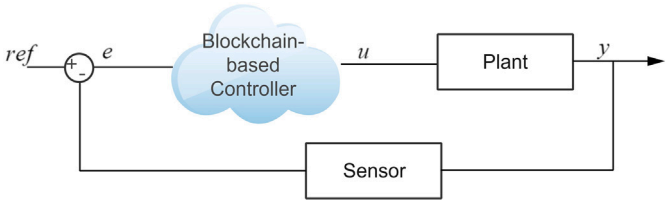

Fig. 4. Control structure of the blockchain-based control system. The controller can be a proportional–integral (PI) or proportional–integral–derivative (PID) implemented as a smart contract. Compared to Fig. 1, where there is no specification on where the cloud controller is hosted and run, the architecture presented here specifies its deployment into a decentralized (blockchain) network.

3.1. Architecture and design

To clearly illustrate the proposed architecture, we describe how a traditional closed-loop control scheme can be reimagined using blockchain technologies. Specifically, our approach relies on deploying controllers as smart contracts within decentralized blockchain networks. Fig. 4 shows a simple structure for the blockchain-based controller in a closed-loop control system. The idea of a blockchain-based cloud controller is that a smart contract including the implementation of a controller of choice (for example, a PID controller), is deployed into a blockchain network.

The smart contract, which encapsulates the controller logic, consists primarily of two core functions:

- Update error: This function receives and securely stores each new error value from the plant. It triggers a blockchain transaction, as it requires writing information in the blockchain and synchronizing all the nodes.
- Compute control action: This function calculates the control output (e.g., a PI control law) based on stored parameters and the most recent error input. The computed output is accessible immediately without triggering further blockchain transactions or incurring additional costs.

These functions ensure that control actions are consistently computed and accessible to users in real-time while maintaining blockchain integrity and transparency.

To illustrate the control algorithm embedded within the smart contract, consider the case of a PI that computes the control action $u(t)$ using the standard discrete-time form:

$$u(t_k) = P + I = K_p e(t_k) + K_i \sum_{j=0}^{k} e(t_j)\,\Delta t \tag{1}$$

where $e(t_k)$ represents the error at discrete time t_k, and K_p, K_i are the proportional and integral gains, respectively. All controller parameters, including gains and sampling intervals, are securely stored within the blockchain, ensuring immutability and transparent auditability.

Fig. 5 shows the architecture of the blockchain-based cloud controller, in which a PI controller is used as an example. The PI controller design is written in a smart contract and deployed into the blockchain network, which requires a transaction. Once the smart contract is deployed, all nodes in the blockchain network have identical copies of the contract and its states; for example, Node 1, Node 2..., Node j..., Node N replicate the PI controller state via a consensus mechanism. At a certain moment, the PI controller logic and state is retrieved from, for instance, Node i (with $1 \le i \le N$), but at a different moment, it can be retrieved from Node j (with $1 \le j \le N$, and j is not necessarily equal to i). In fact, the same control process could get a control action at time t from Node i and the following control action (at $t + \delta$) from Node j.

Given the decentralized replication of controller states, an effective mechanism for accessing these controllers becomes crucial. Therefore, the access to the logic and state of a smart contract (and so, to a blockchain-based cloud controller) is based on a block identification, namely, the hexadecimal address of the smart contract (for example, $0xCF69$... in the example illustrated in Fig. 5). This identifier is used by the application that needs to get the cloud controller service. Due to the distributed network, failures or attacks of multiple nodes will not affect the operation of a blockchain-based controller.

Each smart contract deployed within the blockchain is executed by the Ethereum Virtual Machine or similar blockchain-specific execution

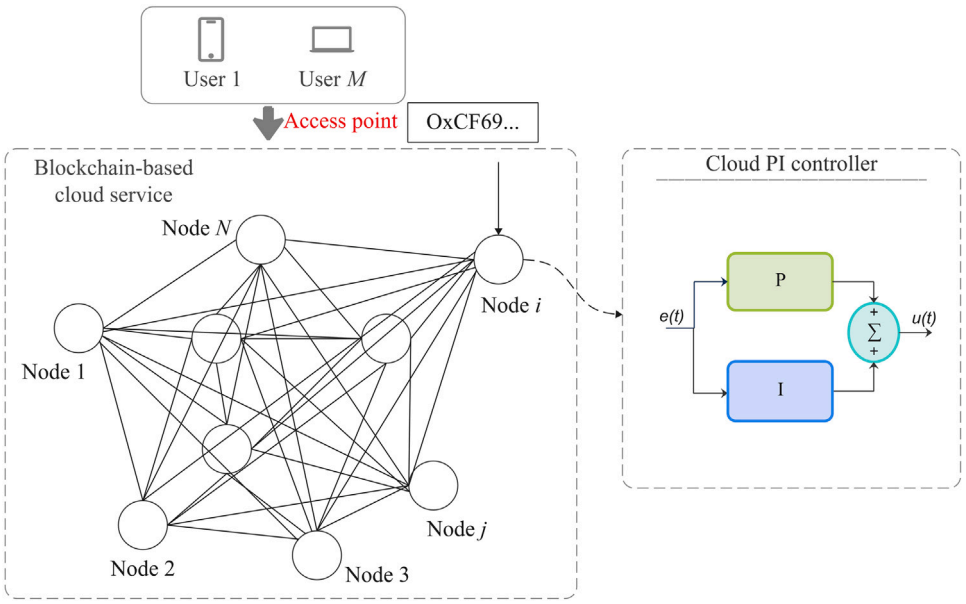

Fig. 5. Architecture of the blockchain-based cloud controller. A PI controller is used as an example. The controller is deployed in the blockchain and made accessible through an hexadecimal address (0xCF69... in this case). Once deployed, all blockchain nodes have identical copies of the smart contract and its states, for example, Node 1, Node 2, etc., can replicate the PI controller state (and action) via consensus.

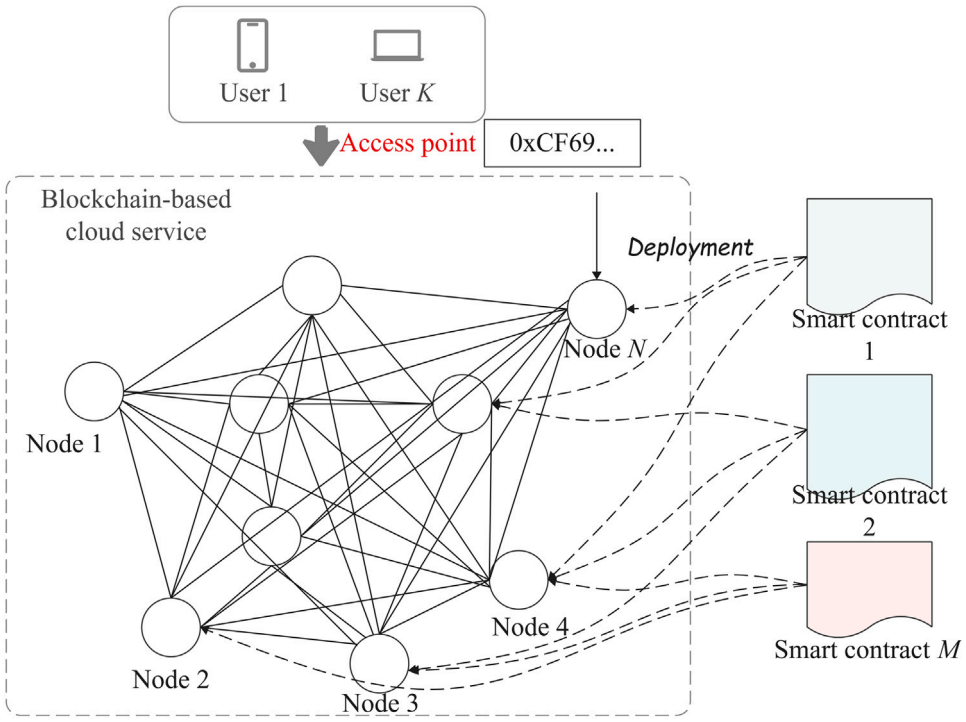

Fig. 6. Deployment of a blockchain based cloud controller using smart contracts. Different smart contracts may contain different types or implementations of controllers (a PI, a PID, a PID with anti-windup, etc.).

environments, ensuring consistent execution across all nodes. Due to the features of being permissionless and open source, anyone can write their smart contracts for controller deployment, or use those from others. Fig. 6 illustrates the deployment of a blockchain-based controller using smart contracts, where the different smart contracts represent different types or implementations of controllers. Therefore, a library of blockchain-based controllers can be provided for international access, as long as a connection to the Internet is available.

To end this section, we evaluate our proposed blockchain-based approach against traditional centralized control architectures and cloud-based solutions. Traditional systems offer optimal latency and performance under ideal conditions but suffer from single points of failure and limited scalability. Cloud-based solutions provide better computational resources and scalability while introducing network dependency and data privacy concerns. Our blockchain-based architecture prioritizes reliability and fault tolerance through decentralization, trading

moderate latency overhead (due to consensus mechanisms) for guaranteed operation continuity during node failure, which is a critical requirement in safety-critical NCSs where downtime is unacceptable. In terms of cost, traditional systems require high upfront hardware investment, and cloud solutions operate on variable pay-per-use models that accumulate subscription fees, whereas blockchain incurs higher initial deployment costs (e.g., smart contract development, multi-node infrastructure) but amortizes long-term operational costs across participants via resource sharing. The integration of EBC and flexible blockchain technology selection (based on Time to Transaction Finality (TTF), requirements) allows our approach to optimize the reliability–performance trade-off for different control applications, making it particularly suitable for multi-stakeholder scenarios requiring high fault tolerance and distributed trust.

3.2. Advantages

The motivation for using cloud controllers based on blockchain technologies can be summarized in the following two categories:

3.2.1. Reliable control

Thanks to the distributed and replication features of blockchain networks, blockchain-based cloud controllers can prevent or reduce some failures in NCSs.

One common source of failure is related to the communications. In [37], the authors categorize the constraints in communications that can lead to failures in NCS in 5: (1) packet loss, (2) variable transmission delays, (3) variable sampling/transmission intervals, (4) quantization errors in transmitted signals, and (5) other communication constraints. While blockchain-based controllers cannot help in the last three points, the first two (packet loss and delays) are mitigated by the fact that all transactions (e.g., control commands) are securely recorded and can be verified and recovered, even if some packets are lost or delayed.

Controllers themselves are another critical source of potential failures. The most obvious one is when there is a power failure affecting the system where the controller runs, and thus it stops being available. Failures or malfunctions within the blockchain-based controller architecture are inherently mitigated by the decentralized replication strategy. Specifically, each node continuously replicates the controller state via consensus mechanisms, ensuring that even if multiple nodes fail or behave maliciously, the system remains operational through unaffected nodes. Detection of node failures occurs naturally as the consensus mechanism will identify and exclude nodes that fail to respond or provide inconsistent data. Such nodes are effectively isolated, maintaining system (and, in this case, control action) integrity.

Another possible source of errors is related to the configuration of the controller (e.g., its tuning parameters). Since blockchain can store configurations and parameter settings in a tamper-proof manner, any changes to these settings can be recorded and verified, ensuring that only authorized and correct configurations are applied. Furthermore, any unauthorized modification attempts of control parameters or historical data trigger cryptographic verification failures, promptly alerting users to potential security breaches.

Beyond configuration-related errors, another critical dimension of reliability pertains to cybersecurity. Network security is also an important factor that has to be considered when trying to prevent or reduce failures in NCSs. In this sense, NCSs are vulnerable to cyber attacks such as denial-of-service, man-in-the-middle attacks, and unauthorized access, which can disrupt the system's operation. Blockchain's decentralized and immutable nature makes it highly resistant to certain types of cyber attacks, such as tampering and unauthorized access. Each transaction is cryptographically secured, and the distributed ledger ensures that any attempt to alter data is quickly detected and prevented.

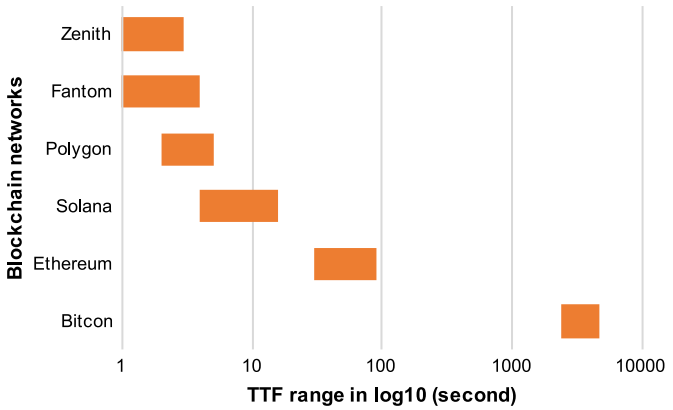

Fig. 7. TTF for different blockchain networks.

3.2.2. Other advantages

Blockchain-based controllers have other advantages, not related to improving the reliability of the system:

(1) *A ready-to-use and worldwide accessible library of controllers*: Due to the open and permissionless nature, anyone can deploy a smart contract and provide controllers for other users, or use those from others. As blockchain contents (including smart contracts) are immutable, all the deployed controllers will live forever in the blockchain. Therefore, multiple different controller implementations will end up being available to the whole world.
(2) *Open source feature*: Anyone can read, copy, modify and redeploy a smart contract. Open source benefits non-programmers and users from different areas to deploy their own controllers much more easily.
(3) *Traceable control actions*: Another crucial feature is that blockchain networks can provide proofs/records for each control action generated from each error signal. This can be used for auditing purposes, for example.

3.3. Drawbacks

While the benefits discussed above clearly demonstrate the value blockchain-based controllers can bring to NCSs, it is equally important to address the practical challenges and limitations that could affect their implementation. The following drawbacks should be carefully considered before applying the proposed solution to NCSs.

(1) Time response: For real-time control systems, the system responses must be in real time, which means that the control actions must be generated fast. However, in addition to network communication constraints, such as time delays and data dropout, blockchain transactions (which are required to generate new control actions) also cost time. The time a transaction takes to be processed, without any possibility of being reverted, is called TTF, and depends on the blockchain network in which the transaction takes place. As we will discuss later, for control systems with time constants smaller than 1 s, current blockchain technologies are (still) not a viable solution for deploying and hosting cloud controllers. However, for process control where time constants are larger, such as temperature control and level control, current TTFs may be acceptable. Moreover, the TTF has decreased sharply during the past few years (see Fig. 7). The TTFs of different blockchain networks vary in a wide range; for example, the average TTF of Fantom ranges from 1 to 3 s, the TTF of Solana ranges from 4 to 12 s, and for Bitcoin, it is around 2400 s. To clearly illustrate the differences with such spread, Fig. 7 represents TTFs on the log10 scale.

(2) Monetary cost: In a blockchain-based controller, there is a monetary cost every time an update is needed in the control action. The

cost can be considered twofold. For the deployment of a controller, a one-time payment is needed, which is notably cheaper than traditional cloud solutions, as this cost may be in the range of just a few dollars to just a few cents, or even less. Therefore, in this sense, the cost is an advantage for a blockchain-based controller when compared to current cloud controllers, where the cost of running a cloud server is usually much higher. However, there is a second monetary cost that has to be considered, associated with its use. As mentioned before, any update in the control action would require a transaction, which implies a cost. Thus, the cost of using a blockchain-based controller per day may be determined as the average cost per transaction multiplied by the average number of control action updates the control system requires per day. Another important consideration is that, while the cost of deploying a controller has to be paid by the agent that deploys it, the cost of using it is paid by the agent that uses it.

(3) Privacy: In addition to the financial and performance considerations, privacy aspects also pose critical challenges for blockchain-based controllers. Transactions and smart contracts' code are public in a blockchain. This means that blockchain-based cloud controllers' code (embedded in smart contracts), tunning parameters (e.g., PID gains, setpoints) and control actions could be visualized by a third agent. While this is normally not an issue, it may be undesirable in certain industrial scenarios, where a control process wants to be kept secret. To prevent this, two solutions are possible: (1) using a private blockchain network, instead of a public one, and (2) applying homomorphic encryption [38] (a form of encryption with an additional evaluation capability for computing over encrypted data) on sensitive data. However, both solutions bring their own disadvantages, which must be considered depending on the use case. Using a private network would eliminate the benefits of advantages 1 and 2 in Section 3.2.2, while using encryption would imply higher delays in the control loop, as data would have to be encrypted and decrypted every time. This highlights a critical trade-off: private blockchains generally provide lower latency and more straightforward privacy controls through permissioned access, but sacrifice the core benefits of public blockchains such as decentralization and openness. Meanwhile, homomorphic encryption enables privacy-preserving computation on public chains but imposes a substantial latency penalty. Moreover, other privacy-preserving mechanisms and system-level security enhancements include the following: (1) Integrating specialized encryption frameworks, such as chaos-based schemes for controller parameter encryption and privacy-preserving smart contracts [39], alongside neural network-based models for securing data streams within the blockchain-based networks [40]; (2) deploying AI-driven intrusion detection systems to monitor smart contract execution anomalies [41]; and (3) adopting lightweight consensus mechanisms to balance latency and security in resource-constrained environments [17].

(4) Smart contract vulnerabilities: Smart contracts are susceptible to errors in their programming logic, potentially exploitable by malicious actors. Common threats include re-entrancy attacks, integer overflow, and logic flaws. Such vulnerabilities may allow unauthorized control actions or data corruption. Rigorous auditing, formal verification, and adhering to secure coding practices are therefore essential prior to deployment.

(5) Threat models for blockchain-based control: Potential attack scenarios include DoS attacks, man-in-the-middle attacks during off-chain interactions, and transaction censorship by malicious nodes. Effective countermeasures include robust node consensus mechanisms, cryptographic authentication methods, and continuous monitoring using AI-driven intrusion detection tools to promptly identify and respond to anomalies.

Table 2
Excluded blockchain network for different process control systems.

Control system examples	Average time constant	Not suitable blockchain networks
Post-combustion CO_2 chemical absorption process [43]	57 min	Bitcoin
The temperature control of a lime kiln [42]	30 min	Bitcoin
Water level control [44]	105 s	Bitcoin
The thermocouple at 700 °C [45]	48.819 s	Bitcoin and Ethereum
Negative-pressure exhaust system of a high-temperature reactor [46]	3 s	Bitcoin, Ethereum, and Solana

4. Applications of blockchain-based cloud controllers in control systems

After detailing the internal logic and on-chain execution of the controller in the previous section, we now focus on how the proposed architecture integrates with real-world networked control systems. This section analyzes how system dynamics, event triggering, and communication constraints are addressed through our implementation. Given the strengths and limitations detailed in the previous sections, we now examine practical considerations for applying the proposed blockchain-based controller architecture to real-world networked control systems. In this section, we explore suitable application scenarios, cost implications, and how EBC strategies can mitigate transaction overhead.

4.1. Control systems suitability

For industrial control processes, the time constant of the systems can vary. Typically, for process control systems (e.g., burning, heat exchange, temperature control, and water level control), such as in thermal power plants (e.g., coal-fired and gas), the time constant is large.

For a control system, a reasonable sampling period, T_s, is approximately 5–10 times lower than the time constant, τ, of such a system [42], which means that $\tau = (5 \sim 10)T_s$. For simplicity, we assume that $T_s \leq \tau$, although for better performance and reliability, $T_s \leq 0.1 * \tau$ should be better considered.

Given these sampling and performance requirements, the TTF becomes a critical parameter for blockchain suitability. Fig. 7 shows the TTF for different blockchain networks. For a blockchain to be used in a control system, the TTF, (T_f), should be smaller than the sampling time T_s ($T_f < T_s$). This would guarantee that $T_f < \tau$, according to the relationship between the sampling period and the time constant. Some examples of control systems are included in Table 2. For the temperature control of a lime kiln, with a time constant of 30 min [42], any blockchain networks from Fig. 7, excluding Bitcoin, can be applied to the control of the system. For a negative-pressure exhaust system of a high-temperature reactor [46], more blockchain networks are excluded, but others, such as Polygon, Fantom and Zenith, can be used for the control. To make it clearer, Table 3 summarizes blockchain suitability for different control processes, considering their typical time constants and associated recommended sampling time.

With a clearer understanding of the types of control systems that are suitable for blockchain-based implementations, we proceed by examining the financial viability and associated transaction costs across different blockchain networks.

Table 3
Blockchain suitability for different control processes.

Blockchain	TTF (s)	Minimum sampling time (s)	Suitable process' time constant (s)	Industrial control example
Ethereum	30–60	$\tau > 60$	$T_s > 300–600$	Liquid level control in big storage tanks
Solana	4–12	$\tau > 12$	$T_s > 60–120$	Temperature control in a calcination furnace
Polygon	2–3	$\tau > 3$	$T_s > 15–30$	Temperature control in food processing
Fantom	1–3	$\tau > 3$	$T_s > 15–30$	Liquid level control in medium to small storage tanks
Zenith	1–2	$\tau > 2$	$T_s > 10–20$	Pressure control in hydraulic systems

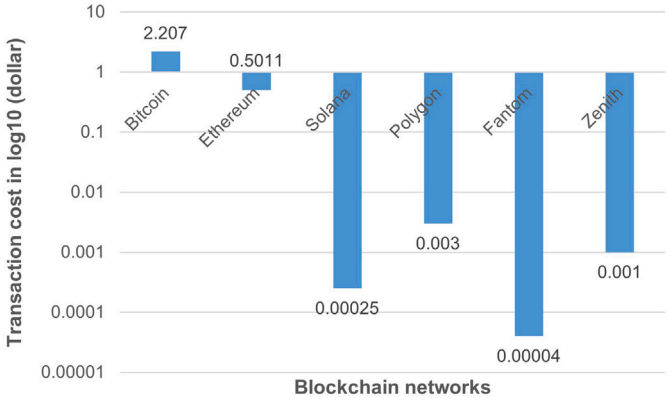

Fig. 8. Transaction cost for different blockchain networks. (Data on 16th November, 2022).

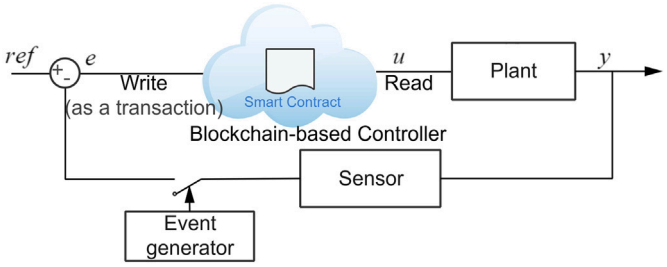

Fig. 9. Event-based control for the blockchain-based cloud control system. This represents an extension of the mechanism illustrated in Fig. 4 in which the feedback loop is only closed when a pre-defined condition is met.

4.2. Costs estimation

As discussed in Section 4.1, several different blockchains can be used in process control systems, depending on the system's time constant. However, the monetary cost of using a blockchain-based controller depends on how many control action updates the system needs on average per unit of time too, so this factor must also be considered. Fig. 8 shows several examples of the transaction costs for different blockchain networks in recent years. Similarly to Fig. 7, the transaction costs also vary in a wide range. To show the costs in a representative way, they are represented on a log10 scale in Fig. 8. Some transaction cost examples are \$2.207 for Bitcoin, \$0.003 for Polygon, and \$0.00004 for Fantom, respectively.

To quantitatively illustrate the economic implications, consider the following simplified calculation for the cost of using a blockchain-based controller:

$$y_{cost} = c_{cpt} * n_t \tag{2}$$

where y_{cost} is the total cost for the control, c_{cpt} is the average cost per transaction (per control action) for a specific blockchain technology, and n_t is the number of transactions, which is also the number of control action updates. It is also important to highlight that in some new blockchain networks, like WAX, the transaction cost is zero.

For the control system example in Table 2 with a time constant of 3 s, according to the TTFs represented in Fig. 7, Polygon, Fantom and Zenith could be used. Taking Polygon as an example, the cost for a single transaction, c_{cpt}, is \$0.003. Therefore, the total cost of the blockchain-based controller service for one day can be calculated according to (2):

$$y_{cost} = 0.003 * 24 * 60 * 60/3 = 86.4\$ \tag{3}$$

However, we can also consider the case of Fantom, for example, where the transaction cost is as low as \$0.00004. In this case, the cost for control is largely reduced to seventy-five times less, meaning around \$1.152 per day.

According to (2), the cost of using a blockchain-based control system can be reduced in two ways: (1) by decreasing the cost per transaction c_{cpt} and/or (2) by decreasing the number of required transactions n_t. While only the first parameter has been considered so far, Section 4.3 analyzes how to further reduce the cost by optimizing the second one.

4.3. Implementation of event-based control

The implementation of EBC emerges as an essential strategy to significantly reduce the number of transactions required in blockchain-based control systems, addressing both the monetary costs and timing constraints identified in previous sections. By triggering control actions only when significant changes occur in system variables, EBC optimizes blockchain interactions, making the proposed approach economically and practically viable for various industrial scenarios. The following section provides a detailed explanation of how this technique integrates into our model.

Here, it is important to remember that in a blockchain-based controller, control action generation requires a transaction execution, while reading a control action occurs in real time and requires no transaction and implies no cost. In this context, EBC can be used to reduce the number of required control action updates without notably degrading the performance of the control system.

In a time-based control system, the control loop is closed on the basis of the sampling period, for example, 0.1 s. While no blockchain would support control action updates every 0.1 s due to their higher current TTFs, even if they do at some point in the future, a blockchain-based control could cost a lot of money. Fig. 9 illustrates how an event-based control would work for a blockchain-based cloud control system. Using EBC, not all error signals are sent to the controller, and so, the control action updates are notably decreased. In this way, n_t can be reduced, and the cost can be further reduced. Moreover, smaller sampling periods, like 0.1 s, which are not supported by current TTF values, would not suppose an issue either. More details on this are given in the case study presented in the next section.

Although time-based blockchain controller applications are firmly limited by the processes' sampling time (as discussed in Section 4.1 and shown in Table 3), when applying EBC in this context, restrictions become more relaxed. By shifting away from strictly time-based updates and towards event-driven triggers, the system no longer requires the blockchain's TTF to strictly comply with the system's sampling time. Instead, it depends on the occurrence of significant events, which is

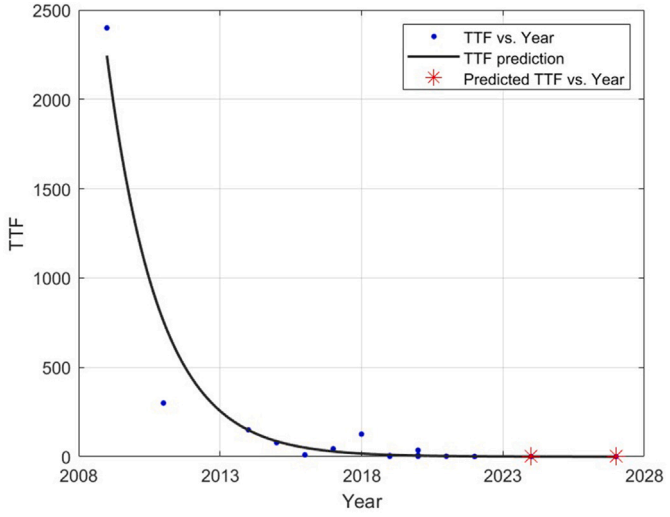

Fig. 10. Prediction of TTF in 2024 and 2027 based on 17 different blockchain networks.

not directly linked to the process time constant (τ), but to the state of the controlled process, meaning that systems that are closer to the stationary state, would require fewer events and thus could tolerate blockchain-based controllers deployed in networks with larger TTFs.

4.4. Future predictions

Considering both current limitations and the potential efficiencies from event-based control, future developments in blockchain performance and cost could significantly expand applicability. In fact,with the advancement of blockchain technologies, TTF and transaction costs are rapidly decreasing to acceptable ranges. This evolution is so fast that we can argue that blockchain networks will soon be suitable to be applied to more industrial control systems with smaller time constants. During the past year, transaction costs have decreased by 16.86% for Bitcoin and 92.19% for Ethereum.[1] Based on the TTF of 17 different blockchain networks, the future TTF can be predicted as shown in Fig. 10 (R^2 = 0.9531). It is estimated that TTF could be as low as 0.6532 s in 2024, and 0.1282 s in 2027. The same prediction can be applied to transaction costs. We can have a reasonable hope that in 5 years, blockchain technologies could even be applied to a system with a time constant of 0.1 s, and the transaction cost, c_{cpt}, could be as low as \$0.0000001. Then, the daily cost for the time-based control of a system with a sampling period of 0.1 s would be \$0.0864.

5. Case study

Having recognized the potential of EBC to minimize transactions and costs, we now detail its practical implementation. To illustrate concretely how this technique significantly optimizes blockchain usage in terms of cost and efficiency, we present a detailed case study focused on a realistic greenhouse climate control scenario.

While time-based control requires transactions to be executed (and paid) every T_s during a day, EBC would only require them when the error is large enough and the system is considered to be outside the stationary state; i.e. when there is a change in the setpoint or when there is a perturbation. Following the example in Section 4.2, this means 24*60*60/3 transactions need to be done/paid every day with the traditional control approach. Instead, with an event-based control, this number could be greatly reduced. The specific amount by which it can be reduced depends mostly on the number of setpoint changes and perturbations that occur during the 24 h.

[1] https://ycharts.com/indicators/categories/cryptocurrency, online; Accessed November 16, 2022.

Table 4
Samples and Thresholds for Time- and Event-Based Control Methods for Different Variables in a Greenhouse Climatic Control System.

Variables	Time-based samples	Threshold δ	Event-based samples
Inside temperature	11 808	0.6	279
Outside temperature	11 808	0.61	353
Humidity	15 360	0.49	358
Solar radiation	15 360	34.30	553
Wind speed	34 560	0.53	3715
Wind direction	34 560	17.84	3255

To further demonstrate the cost efficiency when applying event-based control in a blockchain-based NCS, the greenhouse climatic control system in [47] is used as an example. Taking into account the most common variables in the system, six variables are selected, as listed in Table 4. In time-based control, we assume that the sampling time, T_s, for *Inside Temperature* and *Outside Temperature* (Group 1) is around 58.5 s, that for *Humidity* and *Solar Radiation* (Group 2) is 45 s, and that for *Wind Speed* and *Wind Direction* (Group 3) is 20 s. To illustrate the concrete operational details of our EBC strategy, we adopt a send-on-delta event-triggered policy, which is defined by the following condition:

$$\left|x\left(t_k\right) - x\left(t_s\right)\right| > \delta \tag{4}$$

where $x\left(t_k\right)$ is the last sampled value of the input signal sent to the controller, $x\left(t_s\right)$ is the current value and δ is the specific threshold.

The thresholds for this case are chosen as 5% of the difference between the maximum and minimum values of the different variables. The data of the eight-day simulation are collected and analyzed. Table 4 shows the samples for the time- and event-based control methods, as well as the thresholds used for each variable. It can be concluded that a total of 11808/15360/34560 control action updates are needed for the time-based control in eight days for three groups of variables, while using EBC, the required control action updates are markedly reduced by around 95% on average.

For the three groups of variables in the greenhouse climate control system, T_s is 58.5, 45, and 20 s, respectively. Therefore, excluding Bitcoin and Ethereum, the other four blockchain networks in Fig. 7 could be used. The transaction costs in Fig. 8 are used for calculation of the monetary cost in Fig. 11. This figure shows, for different blockchain networks, the monetary cost for the greenhouse climate control system for eight days using EBC (solid lines) and time-based control (dashed lines). These values are represented on a log10 scale. It can be seen that time-based control is much more costly than EBC for every variable.

6. Conclusion

Having illustrated the feasibility and benefits of our blockchain-based cloud controller through both theoretical analysis and a practical application example, we summarize our findings and outline directions for future research in the following concluding remarks.

This article considers blockchain-based cloud controllers for reliable control in NCSs, using smart contracts for controller deployment. The architecture, design, and deployment of the proposed blockchain-based controller are presented, and its advantages and drawbacks are discussed. The proposed solution can provide reliable controllers for NCSs and a library of controllers that are ready to use and worldwide accessible with open source features. With relatively slower TTFs for current blockchain networks, the proposed solution can be used in process control systems with large time constants, such as temperature control or level control systems. However, with the rapid advances in blockchain technologies, transaction costs and times are expected

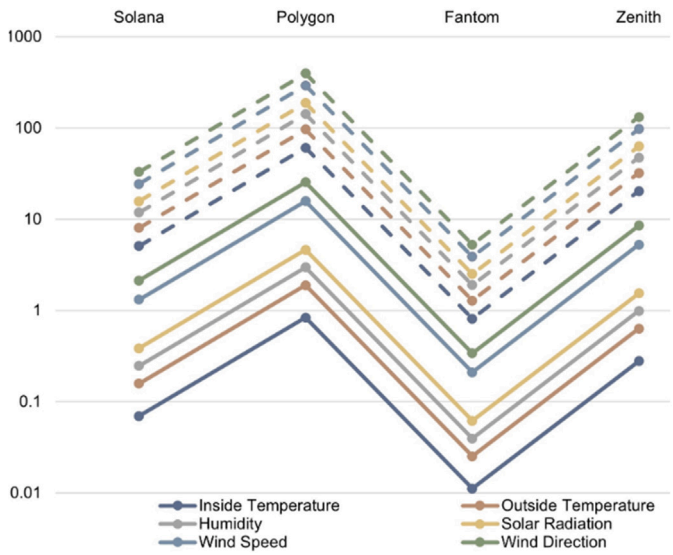

Fig. 11. Estimation of the monetary cost of different blockchain networks (Solana, Polygon, Fantom and Zenith) for the greenhouse climatic control system in eight days using EBC (solid lines) and time-based control (dashed lines) methods.

to decrease even more, which will benefit the use of the proposed NCSs solution in terms of monetary cost and the variety of processes to which it could be applied. Moreover, through the adoption of EBC not only could systems with faster dynamics and lower time constants be supported, but, as the case study indicates, the cost of the proposed solution can also be significantly decreased.

Future work will focus on: (1) programming a PI controller, (2) deploying it as a smart contract in one, or more, of the considered blockchain networks, (3) using it to control a real temperature and/or liquid level process, and (4) evaluating its performance, for example, stability under node failures and TTF compliance, in this/these real scenarios. Building upon this foundation, we propose the following strategic research agenda: (1) Development of consensus mechanisms for coordinating decentralized controllers to achieve system-wide control objectives, (2) Integration of federated learning algorithms with smart contracts to enable privacy-preserving collaborative adaptation using distributed data, (3) Rigorous testing in hybrid IoT-blockchain environments to validate latency, resilience and security, and (4) address the economic dimension of the proposed architecture in greater depth by incorporating statistical analysis and sensitivity studies of blockchain transaction costs (which includes exploring cost variability across time, network congestion conditions, and platforms, as well as validating cost-performance trade-offs via significance testing).

CRediT authorship contribution statement

Zhongcheng Lei: Writing – review & editing, Writing – original draft, Validation, Investigation, Funding acquisition. **Luis de la Torre:** Writing – review & editing, Methodology, Investigation, Funding acquisition, Conceptualization. **Francisco-José Mañas-Álvarez:** Writing – review & editing, Validation, Methodology. **Wenshan Hu:** Supervision, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant 62103308 and Grant 62073247, in part by the Fundamental Research Funds for the Central Universities under Grant 2042023kf0095, in part by the Agencia Estatal de Investigación (AEI) under Project PID2022-139187OB-I00, in part by the Natural Science Foundation of Hubei Province of China under Grant 2024AFB719, and in part by the China Scholarship Council (CSC) under Grant 202106275005.

Data availability

No data was used for the research described in the article.

References

[1] X.-M. Sun, G.-P. Liu, D. Rees, W. Wang, Stability of systems with controller failure and time-varying delay, IEEE Trans. Autom. Control 53 (10) (2008) 2391–2396.
[2] G. Zhai, H. Lin, Controller failure time analysis for symmetric control systems, Internat. J. Control 77 (6) (2004) 598–605.
[3] X. Huang, Y. Yan, Output feedback control of underactuated spacecraft hovering in circular orbit with radial or in-track controller failure, IEEE Trans. Ind. Electron. 63 (9) (2016) 5569–5581.
[4] X.-M. Zhang, Q.-L. Han, B.-L. Zhang, An overview and deep investigation on sampled-data-based event-triggered control and filtering for networked systems, IEEE Trans. Ind. Inform. 13 (1) (2017) 4–16.
[5] L. de la Torre, J. Chacon, D. Chaos, S. Dormido, J. Sanchez, Using server-sent events for event-based control laboratory practices in distance and blended learning, in: 2019 18th Eur. Control Conf., ECC, 2019, pp. 3053–3058.
[6] G.-P. Liu, Predictive control of networked multiagent systems via cloud computing, IEEE Trans. Cybern. 47 (8) (2017) 1852–1859.
[7] V. Natanelov, S. Cao, M. Foth, U. Dulleck, Blockchain smart contracts for supply chain finance: Mapping the innovation potential in Australia-China beef supply chains, J. Ind. Inf. Integr. 30 (2022) 100389.
[8] M.M. Nuttah, P. Roma, G.L. Nigro, G. Perrone, Understanding blockchain applications in industry 4.0: From information technology to manufacturing and operations management, J. Ind. Inf. Integr. 33 (2023) 100456.
[9] K. Hameed, M. Barika, S. Garg, M.B. Amin, B. Kang, A taxonomy study on securing blockchain-based industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues, J. Ind. Inf. Integr. 26 (2022) 100312.
[10] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, Y. Ma, Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities, IEEE Commun. Mag. 56 (7) (2018) 82–88.

[11] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, Z. Zou, A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things, J. Ind. Inf. Integr. 21 (2021) 100190.
[12] S. Suhail, M. Iqbal, R. Hussain, S.U.R. Malik, R. Jurdak, Triple: A blockchain-based digital twin framework for cyber–physical systems security, J. Ind. Inf. Integr. 42 (2024) 100706.
[13] J.L.R. Villalon, L. de la Torre, Z. Lei, W. Hu, H.T. Kussaba, V. Lemieux, A decentralised approach to cyber–physical systems as a service: Managing shared access worldwide through blockchain standards, Comput. Ind. 167 (2025) 104264.
[14] Y. Yu, G.-P. Liu, X. Zhou, W. Hu, Blockchain protocol-based predictive secure control for networked systems, IEEE Trans. Ind. Electron. 70 (1) (2023) 783–792.
[15] Y. Yu, G.-P. Liu, H. Xiao, W. Hu, Design of networked secure and real-time control based on blockchain techniques, IEEE Trans. Ind. Electron. 69 (4) (2022) 4096–4106.
[16] M.v. Ould Mohamed, A blockchain-based approach to secure networked control systems against false data injection attacks, J. Electr. Eng. Technol. 18 (3) (2023) 2335–2342.
[17] A.A. Khan, S. Dhabi, J. Yang, W. Alhakami, S. Bourouis, L. Yee, B-LPoET: A middleware lightweight proof-of-elapsed time (poet) for efficient distributed transaction execution and security on blockchain using multithreading technology, Comput. Electr. Eng. 118 (2024) 109343.
[18] A.A. Khan, J. Yang, A.A. Laghari, A.M. Baqasah, R. Alroobaea, C.S. Ku, R. Alizadehsani, U.R. Acharya, L.Y. Por, Baiot-ems: Consortium network for small-medium enterprises management system with blockchain and augmented intelligence of things, Eng. Appl. Artif. Intell. 141 (2025) 109838.
[19] Permissionless innovation, 2022, https://files.iota.org/comms/IOTA_for_Business.pdf, online; (Accessed 12 December 2022).
[20] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008, https://bitcoin.org/bitcoin.pdf, online; (Accessed 12 December 2022).
[21] Introduction to smart contracts, 2022, https://ethereum.org/en/smart-contracts/, online; (Accessed 25 November 2022).
[22] H. Wang, C. Guo, S. Cheng, Loc—a new financial loan management system based on smart contracts, Future Gener. Comput. Syst. 100 (2019) 648–655.
[23] O. Novo, Blockchain meets IoT: An architecture for scalable access management in IoT, IEEE Internet Things J. 5 (2) (2018) 1184–1195.
[24] D. Kirli, B. Couraud, V. Robu, M. Salgado-Bravo, S. Norbu, M. Andoni, I. Antonopoulos, M. Negrete-Pincetic, D. Flynn, A. Kiprakis, Smart contracts in energy systems: A systematic review of fundamental approaches and implementations, Renew. Sustain. Energy Rev. 158 (2022) 112013.
[25] J. Sedlmeir, H.U. Buhl, G. Fridgen, R. Keller, The energy consumption of blockchain technology: Beyond myth, Bus. Inf. Syst. Eng. 62 (6) (2020) 599–608.
[26] Ethereum whitepaper, 2022, https://ethereum.org/en/whitepaper/, online; (Accessed 12 December 2022).
[27] M. Zamani, M. Movahedi, M. Raykova, Rapidchain: Scaling blockchain via full sharding, in: Proc. ACM Conf. Computer Commun. Secur., 2018, pp. 931–948.
[28] A.H. Karbasi, S. Shahpasand, A post-quantum end-to-end encryption over smart contract-based blockchain for defeating man-in-the-middle and interception attacks, Peer-to-Peer Netw. Appl. 13 (5) (2020) 1423–1441.
[29] M. Singh, G.S. Aujla, A. Singh, N. Kumar, S. Garg, Deep-learning-based blockchain framework for secure software-defined industrial networks, IEEE Trans. Ind. Inform. 17 (1) (2021) 606–616.
[30] D. Hawashin, M. Nemer, K. Salah, R. Jayaraman, D. Svetinovic, E. Damiani, Blockchain and nft-based traceability and certification for uav parts in manufacturing, J. Ind. Inf. Integr. 39 (2024) 100597.
[31] Solana: A new architecture for a high performance blockchain v0.8.13, 2022, https://solana.com/solana-whitepaper.pdf, online; (Accessed 12 December 2022).
[32] Polygon: Ethereum's internet of blockchains, 2022, https://bumba.global/assets/whitepaper/Polygon.pdf, online; (Accessed 12 December 2022).
[33] W. Quigley, J. Yantis, L. Sliwka, M. CasSelle, WAX protocol white paper, 2019, https://github.com/worldwide-asset-exchange/whitepaper, online; (Accessed 12 December 2022).
[34] Fantom whitepaper, 2018, https://fantom.foundation/_next/static/media/wp_fantom_v1.6.39329cdc5d0ee59684cbc6f228516383.pdf, online; (Accessed 12 December 2022).
[35] Welcome to the Casper network, 2022, https://docs.casper.network/, online; (Accessed 12 December 2022).
[36] Zenith whitepaper, 2022, https://docs.zenithchain.co/whitepaper, online; (Accessed 12 December 2022).
[37] M.S. Mahmoud, M.M. Hamdan, Fundamental issues in networked control systems, IEEE/CAA J. Autom. Sin. 5 (5) (2018) 902–922.
[38] C. Gentry, Fully homomorphic encryption using ideal lattices, in: Proc. Annu. ACM Symp. Theory Comput., 2009, pp. 169–178.
[39] W. Alexan, Y.-L. Chen, L.Y. Por, M. Gabr, Hyperchaotic maps and the single neuron model: A novel framework for chaos-based image encryption, Symmetry 15 (5) (2023).
[40] M. Gabr, A. Diab, H.T. Elshoush, Y.-L. Chen, L.Y. Por, C.S. Ku, W. Alexan, Data security utilizing a memristive coupled neural network in 3d models, IEEE Access 12 (2024) 116457–116477.
[41] J. Yang, Y. Wu, Y. Yuan, H. Xue, S. Bourouis, M. Abdel-Salam, S. Prajapat, L.Y. Por, LLM-AE-MP: Web attack detection using a large language model with autoencoder and multilayer perceptron, Expert Syst. Appl. 274 (2025) 126982.
[42] A. Horch, A.J. Isaksson, A modified index for control performance assessment, J. Process Control 9 (6) (1999) 475–483.
[43] A. Lawal, M. Wang, P. Stephenson, G. Koumpouras, H. Yeung, Dynamic modelling and analysis of post-combustion co2 chemical absorption process for coal-fired power plants, Fuel 89 (10) (2010) 2791–2801.
[44] T.S. Ng, Process control, in: Real Time Control Engineering: Systems and Automation, Springer Singapore, Singapore, 2016, pp. 115–120.
[45] Y. Li, Z. Zhang, X. Hao, W. Yin, A measurement system for time constant of thermocouple sensor based on high temperature furnace, Appl. Sci. 8 (12) (2018) 2585.
[46] R. Du, Z. Zhang, F. Jiang, Simulation-aided design of the negative-pressure exhaust system in htgr nuclear power plants, Nucl. Eng. Des. 343 (2019) 43–56.
[47] A. Pawlowski, J.L. Guzmán, F. Rodríguez, M. Berenguel, J. Sanchez, S. Dormido, Event-based control and wireless sensor network for greenhouse diurnal temperature control: A simulated case study, in: IEEE Symp. Emerging. Technol. Fact. Autom., 2008, pp. 500–507.